Attachment 1

SYSTEM SAFETY ENGINEERING PROCESS[1]

1.0 INTRODUCTION

The System Safety Engineering Process has been defined as the application of system safety engineering and management principles, operational standards, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system's life cycle. Within this definition resides four explicit and one implicit major components. The four explicit components are:

1. System Safety Engineering
2. System Safety Management
3. The System Life Cycle
4. The System

The implicit component is the System Safety Program.

1.1 DEFINITIONS

1.1.1 System A system may be defined as a composite structure of personnel, procedures, materials, tools, equipment, facilities, and software integrated, through the application of sound systems engineering processes and practices, into a designed format to efficiently and effectively accomplish a predetermined objective.

1.1.2 System Life Cycle A system's Life Cycle can be separated into six (6) distinct phases starting with conception and terminating with disposition. Those 6-phases are:

1. Conception
2. Research and Development (R&D)
3. Design
4. Deployment
5. Operation
6. Disposition

1.1.3 System Safety Management System Safety Management defines the system safety program requirements and ensures the planning, implementation and accomplishment of the identified system safety tasks and activities within the scope of the overall system design, engineering, and integration program.

1.1.4 System Safety Engineering System Safety Engineering is the application of scientific and engineering principles, criteria, and techniques necessary to identify and

[1] The following documentation incorporates sections, paragraphs and passages from both Military Standard 882 and the Systems Safety Manual (System Safety Society Standard)

eliminate hazards or reduce the probability of their occurrence, and the associated risk . System Safety engineering performs those system safety tasks and activities identified by System Safety Management.

1.1.5 System Safety Program The implicit component of the System Safety Engineering Process is the definition and implementation of a System Safety Program. Military Standard (Mil Std) 882, System Safety Program Requirements, defines a system safety program as:

> "The combined tasks and activities of system safety management and system safety engineering that enhance operational effectiveness by satisfying the system safety requirements in a timely, cost-effective manner throughout all phases of the system life cycle."

The objectives of a system safety program are to ensure that:

a. Safety, consistent with overall system objectives and requirements, is designed into the system in a efficient and cost effective manner.

b. Hazards associated with the form, fit, function, operation, and support of the system are identified, evaluated, and eliminated, or the associated risk reduced to acceptable levels throughout its entire life cycle.

c. Safety data, including lessons learned from similar systems are identified and applied.

d. The proper safety evaluation and analytical techniques are selected and applied to new designs, materials, processes, and procedures to minimize the associated risk.

e. All methods employed to eliminate hazards and reduce risks, and their effectiveness, are properly applied and documented.

f. Design changes required to meet specified levels of risk are minimized through the efficient and effective application of safety features during the R&D or acquisition[2] phase of the system.

g. Changes in system design, configuration, or application are evaluated and analyzed for impacts to overall system safety and the established acceptable level of risk.

h. Environmental concerns and impacts associated with the use or disposal of hazardous materials are identified and provided for.

i. Data banks are established to ensure that significant safety data is retained and readily available for trend analysis.

---

[2] It is not uncommon to find that it is more cost effective to acquire a system, major component (subsystem) or support and test equipment (S&TE). From the end user's perspective, it is a purchase or acquisition. Within the System Life Cycle, the design phase becomes the acquisition phase.

The methodology by which the System Safety Program and System Safety Engineering Process is defined and implemented is the System Safety Program Plan.

1.1.6 System Safety Program Plan The System Safety Program Plan provides a description of the planned methods by which recognized and accepted safety standards and requirements, including organizational responsibilities, resources, methods of accomplishment, milestones, and levels of effort, are to be tailored and integration with other system engineering functions to ensure hazards are identified and eliminated, or that their probability of occurrence is reduced to acceptable levels of risk. Tailoring refers to the selection and application of recognized and accepted safety standards, requirements, and procedures that are necessary, appropriate, and consistent with overall system objectives. Integration refers to the application of hazard elimination and reduction techniques in a manner that complements or enhances the implementation of the other system engineering functions.

2.0 APPLICATION

It can be stated, in general terms, that the intent of the System Safety Engineering Process is to identify and eliminate, or reduce or control hazards to acceptable levels of risk throughout a system's life cycle. Hazard reduction or control is commonly referred to as mitigation; i.e. reduce or moderate the effect thereof. This requires an understanding of terminology associated with the word "hazard" as it is used in this document.

2.1 HAZARD DEFINITIONS

The following definition of hazard and associated terms have been taken from Mil Std 882:

2.1.1 Hazard A condition that is a prerequisite to a mishap.

2.1.2 Mishap An unplanned event or series of events that results in death, injury, occupational illness, or damage to or loss of equipment or property.

2.1.3 Hazardous Event An occurrence that creates a hazard.

2.1.4 Hazard Probability The aggregate probability of occurrence of the individual hazardous event that create a specific hazard. The probability that a hazard will be created during the planned life expectancy of a system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning hazard probabilities should be documented in hazard analysis reports. The terminology is commonly applied to qualitative hazard probability assessments:

2.1.4.1 <u>Frequent</u> Likely to occur frequently; commonly experienced.

2.1.4.2 Probable Will occur several times in the system's life cycle.

2.1.4.3 Occasional Likely to occur sometime in the system's life cycle.

2.1.4.4 Remote Unlikely but possible to occur sometime in the system's life cycle.

2.1.4.5 Improbable So unlikely, it can be assumed the occurrence may not be experienced.

2.1.5 Hazardous Event Probability The likelihood, expressed in quantitative or qualitative terms, that a hazardous event will occur.

2.1.6 Hazard Severity An assessment of the worst credible mishap that could be caused by a specific hazard. Hazard severity categories are defined to provide a qualitative measure of the worse credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction as follows:

2.1.6.1 Catastrophic Death or system loss.

2.1.6.2 Critical Severe injury or occupational illness; severe system damage.

2.1.6.3 Marginal Minor injury or occupational illness; minor system damage.

2.1.6.4 Negligible Less than minor injury or occupational illness; or less than minor system damage.

2.2. CONCEPTUAL PHASE

During the Conceptual Phase, safety standards, specifications, regulations, and relevant system safety design requirements are identified and evaluated for relevance and applicability. It is during this phase that System Safety Management develops and System Safety Engineering initiates implementation of the System Safety Program Plan (SSPP) which, at a minimum, should define:

a. The Purpose, Scope and Objectives of the SSPP.

b. The System Safety Organization including all interfaces and Working Group.

c. System Safety Program Reviews and Milestones.

d. General System Safety Requirements and Operational Standards.

e. Hazard Analyses.

f. System Safety Data and Assessments.

g. Safety Compliance Assessment.

h. Safety Review of Engineering Change Proposals and Deviation/Waiver Request.

i. Safety Program Verification, Validation and Auditing.

j. Safety Training

k. Mishap and Hazardous Malfunction Analysis and Reporting.

2.3 R&D PHASE

During the R&D phase, those safety standards, specifications, regulations, and relevant system safety design requirements identified as relevant or applicable during the Conceptual Phase are evaluated against design documentation and developmental hardware for the purpose of:

a. Eliminating hazards or reducing the associated risk through design, material selection, or substitution.

b. Identifying and isolating hazardous materials and operations.

c. Positioning components so that access during operations, servicing, or maintenance minimizes personnel exposure to hazardous conditions or situations.

d. Minimizing risk due to extreme temperatures, pressure, noise, or toxicity, accelerations or vibrations.

e. Eliminating or mitigating risk due to human factors.

f. Mitigating or controlling damage due to component failure.

g. Providing system and personnel protection by utilizing emergency systems or devices.

h. Minimizing the severity of personnel injury or system damage in the event of a mishap.

i. Incorporating software controlled or monitored functions to minimize initiation of hazardous events or mishaps.

2.3.1 Preliminary Hazard List (PHL)

A byproduct of the Conceptual Phase that is fully implemented and utilized during the R&D Phase is the PHL. The PHL is used to document those possible hazards identified as being applicable to or inherent in the design to ensure their recognition, visibility and investigation. The PHL may also identify hazards that require special safety design

emphasis or hazardous areas where in-depth safety analyses are needed as well as the scope of those analyses. At a minimum, the PHL should identify:

- The Hazard
- When identified (phase of system life cycle)[3]
- How (regulation, specification, requirement, analysis, malfunction, failure) and by whom.
- Severity and Probability of Occurrence.
- Probable/actual cause(s)
- Proposed elimination/mitigation techniques.
- Status (Open-action pending /Closed-eliminated/Mitigated
- Process of elimination/mitigation.
- Oversight/approval authority.

2.3.2 Preliminary Hazard Analysis (PHA)

The PHA is the initial effort relative to the conduct of hazard analyses. The purpose of the PHA is not to affect control of all risks but to fully recognize the hazardous states and all of the associated risks. It is the basic hazard analysis which establishes the framework for other hazard analyses which may be performed. The output of the PHA may also be used to develop system safety requirements and design specifications. The PHA will usually include, but is not limited to, the identification and analysis of:

a. Hazardous components such as fuels, propellants, lasers, explosives, toxic substances, pressure systems and other energy sources.

b. Safety related interfaces, material incompatibilities, electromagnetic interference (EMI), inadvertent activation, fire/explosion initiation and propagation, and hardware and software controls.

c. Environmental constraints including the operating environments, exposure to toxic substances, health hazards, fire, electrostatic discharge (ESD), lightning, ionizing and non-ionizing radiation.

d. Operating, test, maintenance and emergency procedures, human factor engineering and human error analysis, life support requirements, human safety systems (egress, rescue, survival), and equipment salvage operations.

e. Facilities, Support and Test Equipment (S&TE), packaging, handling, storage, and transportation (PHS&T) requirements, provisions for storage, assembly, checkout,

[3] The PHL is converted to a System Hazard List (SHL) and is used as a device for tracking a hazard through the cycle of identification, classification, evaluation, analysis, elimination or mitigation, and elimination/mitigation verification and validation or residual risk acceptance.

and testing of hazardous systems/ subsystems/assemblies/subassemblies which contain, control or monitor toxic, flammable, explosive, corrosive or cryogenic fluids; radiation or noise emitters or other power/energy sources.

f. Training and certification/qualification requirements pertaining to hazardous operations and abatement; and safety operations, maintenance, control, supervision.

g. Essential safety related equipment, safeguards and the application of interlocks, redundancy, hardware/software fail safe design considerations, subsystem/assembly protection, fire suppression system, personal protective equipment, and noise or radiation barriers.

Some specialized safety analyses that may be employed in support of the PHA are:

2.3.2.1 Comparison-To-Criteria (CTC) Analysis The purpose of the CTC Analysis is to provide a formal and structured format that identifies all safety requirements for a system and ensures compliance with those requirements.

2.3.2.2 Environmental Risk Analysis The purpose of Environmental Risk Analysis is to assess the risk of environmental non-compliance that may be caused by a failure in a system.

2.3.2.3 External Events Analysis The purpose of this analysis is to focus the attention of the system safety analyst to those events outside the system under examination. It is to further hypothesize the range of credible events that may have an effect on the system being examined.

2.3.2.4 Fire Hazard Analyses There are multiple types of fire hazard analyses, four of which are described below:

2.3.2.4.1 Preliminary Fire-Hazard Analysis This type of analysis presents a listing of what are believed to be the primary fire hazards of concern, together with a qualitative estimate of the potential effects of these hazards on safety systems and the "best method" to control the hazard.

2.3.2.4.2 Barrier Analysis An analysis technique which describes fire severity in terms of total involvement of combustibles in a room and in terms of total involvement effect on the room's structural integrity. Total involvement of combustibles is often referred to as "flashover."

2.3.2.4.3 Fuel Load Analysis As described in the National Fire Protection Association (NFPA) Handbook, a fuel load analysis starts by adding up the weight of combustibles in a room and converting the weight to energy content of the fuel per unit floor area. The measured fuel load is then compared to a linear fire-duration scale.

2.3.2.4.4 National Fire Protection Association Decision Tree Analysis This method views fire events in a logical sequence leading to a predefined fire objective for life safety and property protection.

2.3.2.5 Health Hazard Assessment (HHA) The purpose of the HHA is to provide a detailed review of hazardous materials used in a facility or operation and to identify and evaluate potential hazards, eliminate or control the hazards, and to provide a verification of health-related requirements. The HHA uses the Material Safety Data Sheet (MSDS) as the primary source and starting place for information on each material within the facility or operation, as well as each material that may be introduced.

2.3.2.6 Laser Safety Analysis The purpose of laser safety analysis is to provide a means to assess the hazards of non-ionizing radiation. As such, its intent is to also identify associated hazards and the types of controls available and required for laser hazards.

2.3.2.7 Management Oversight and Risk Tree (MORT) Analysis The purpose of the MORT technique is to systematically and logically analyze a system or an accident in order to examine and determine detailed information about the process inner-workings to include identification of hazards. It applies a pre-designed, systematized logic tree to the identification of total system risk, both those inherent in physical equipment and processes and those which arise from operational/management inadequacies. The pre-designed tree, intended as a comparison tool, generally describes all phases of a safety program and is applicable to systems and processes of all kinds. The technique is of particular value in accident/incident investigation as a means of discovering system or program weaknesses or errors which provide an environment conducive to mishaps.

2.3.2.8 Nuclear Safety/Cross-Check Analyses These analyses are applicable to reactor and non-reactor nuclear system.

2.3.2.8 1 Nuclear Safety Analyses The purpose of the nuclear safety analysis is to establish requirements for contractors responsible for the design, construction, operation, decontamination, or decommissioning of nuclear facilities or equipment to develop safety analyses that establish and evaluate the adequacy of the safety bases of the facility/equipment. The Department of Energy (DOE) requires that the safety bases analyzed include management, design, construction, operation, and engineering characteristics necessary to protect the public, workers, and the environment from the safety and health hazards posed by the nuclear facility or non-facility nuclear operations. The Nuclear Safety Analysis Report (NSAR) documents the results of the analysis.

2.3.2.8.2 Nuclear Safety Cross-Check Analyses (NSCCA) The NSCCA provides a technique that verifies and validates software designs. The NSCCA is also a reliability hazard assessment method that is traceable to requirements-based testing.

2.3.2.9 Probabilistic Risk Assessment (PRA) The PRA provides an analysis technique for low probability, but catastrophic severity type events. It identifies and delineates the combinations of events that, if they occur, will lead to an accident and estimates the frequency of occurrence for each combination of events, and then estimates the

consequences. It involves developing models of the system, data bases giving competent failure rates, and baselines of the dominant risk sequences.

2.3.2.10 Single-Point Failure Analysis (SPFA) The purpose of a SPFA is to identify those failures that would produce a catastrophic event in terms of injury or monetary loss if they were to occur by themselves. The SFFA is performed by examining the system, element by element, and identifying those discrete elements or interfaces whose malfunction or failure, taken individually, would induce system failure. The technique is equally applicable to hardware, software and formalized human operator procedures.

2.3.2.11 Explosive Safety Analysis The purpose of an explosive safety analysis is to provide an assessment of the hazards and potential explosive effects of the storage, handling or operations with various types of explosives from gram to ton quantities and to determine the damage potential.

An output of the PHA, SHA, and Safety Program Reviews is the Safety Assessment Report.

2.3.3 Safety Assessment Report (SAR).

The purpose of the SAR is to identify and document:

a. The safety features of the hardware, software, and system design;

b. The operational and procedural hazards that may be present including the specific controls and associated precautions;

c. The safety criteria and methodology used to classify and rank hazards;

d. The analyses and tests performed to identify hazards inherent in the system including:

    1. Hazards that still have residual risk, and the actions that have been taken to reduce the associated risk to specified acceptable levels.

    2. Results of tests conducted to verify and validate safety criteria requirements and analyses.

e. The results of the safety program efforts;

f. All significant hazards, the operating conditions (normal or abnormal) when they can be expected to occur, and specific recommendations or precautions required to ensure safety of personnel and property.

g. All hazardous materials generated by or used in the system, including:

    1. Identification by type, quantity, and potential hazards.

2. Safety precautions and procedures necessary during PHS&T).

3. Explosives hazard classifications and Material Safety Data Sheets.

h. The environmental impacts or hazards associated with the deployment, operation (including logistical support) and disposition of the system;

i. A signed statement by the System Safety Program Manager attesting to the fact that all identified hazards have been eliminated or their associated risks controlled to levels specified as acceptable, and that the system is ready to test or operate or proceed to the next design/acquisition or life cycle phase.

2.4 DESIGN PHASE

The Design Phase of the System Engineering and Integration Process is subdivided into phases punctuated by Design Reviews. The purpose of the Design Reviews are primarily to assure management that the program is on schedule, that all critical issues have been identified and have either been resolved or that the proposed solutions are "workable". The number and frequency of design reviews will vary according to the complexity of the system and the results of the previous review. A simple system or an "off-the-shelf" acquisition may have only one. Conversely, a "typical" three phase design review process, consisting of a conceptual, preliminary and critical design review, may have those reviews subdivided into phases, identified as Phase I, II, and III, as well.

During this phase of system development or acquisition, hazards identified by the PHA are evaluated and analyzed for inadequate safety features or induced hazards, and follow-on safety evaluations and analyses are conducted, and safety related design changes are recommended, documented, tracked, verified, and validated. The major follow-on safety analyses initiated, but not necessarily completed during this phase are the:

a. System Hazard Analysis (SHA);

b. Subsystem Hazard Analysis (SSHA);

c. Software Hazard Analysis (SWHA); and

d. Operating and Support Hazard Analysis (O&SHA).

2.4.1. System Hazard Analysis (SHA) The SHA, in many respects, is a continuation of the PHA in that most often the emphasis of the PHA is hazard identification which will include an intuitive estimate of the severity and probability of occurrence. The SHA will verify and validate the results of the PHA or eliminate some of the identified hazards as not being applicable to the design or as having been addressed and eliminated by design. It may also result in some of the PHA hazards being upgraded or downgraded in severity or probability of occurrence due to design considerations. However, since the design has reach a higher level of detail and sophistication, new hazards will be identified and rated as well.

Depending on the characteristics of the system, specialized analysis will be used to support or complement the SHA. Some of the most common specialized analysis are:

2.4.1.1. Bent Pin Analysis This analysis investigates the faults that can result from bent pins in electrical connectors and is applicable to the SHA, SSHA, and O&SHA during maintenance operations.

2.4.1.2 Change Analysis Change analysis examines the potential effects of modification from a starting point on baseline.. The change analysis systematically hypothesizes worst-case effects from each modification from that baseline.

2.4.1.3 Checklist Analysis A list of specific items is used to identify known types of hazards, design deficiencies, and potential accident situations associated with common equipment and operations. the identified items are compared to appropriate standards. The Checklist Analysis technique can be used to evaluate materials, equipment, or procedures.

2.4.1.4 Contingency Analysis A contingency analysis is a method of preparation for emergencies by identifying potential accident causing conditions and respective mitigating measures to include protective systems and equipment.

2.4.1.5 Cryogenic Systems Safety Analysis (CSSA) The purpose of the CSSA is to specifically examine cryogenic systems from a safety standpoint in order to eliminate or to mitigate the hazardous effects of potentially hazardous materials at extremely low temperatures.

2.4.1.6 Event/Fault Tree Analyses

2.4.1.6.1 Event Tree Analysis (ETA) The ETA is an analytical tool that can be used to organize, characterize, and quantify potential accidents in a methodical manner. An event tree models the sequence of events that results from a single initiating event.

2.4.1.6.2 Fault Tree Analysis (FTA) The purpose of the FTA is to assess a system by identifying a postulated undesirable end event and examining the range of potential events that could lead to that state or condition. The FTA can model the failure of a single event or multiple failures which lead to a single system failure. The FTA is a Top Down analysis versus the Bottom Up approach for the event tree analysis.

2.4.1.7 Facilities System Safety Analysis (FSSA) The purpose of the FSSA is to apply system safety analysis techniques to a facility and its operations. Safety analyses, within the FSSA, document the safety bases for and commitments to the control of subsequent operations. This includes staffing and qualification of operating crews; the development, testing, validation, and in-service refinement of procedures and personnel training materials; and the safety analysis of the person-machine interface for operations and maintenance. In safety analyses for new facilities and safety-significant modifications to existing facilities, considerations of reliable operations, surveillance, and maintenance and the associated human factors safety analysis are developed in parallel and integrated with hardware safety design and analysis. Once a facility or operation is in service, the

responsible contractor and safety oversight activities use the report, which contains OSHA 1910.119 Program Requirements.

2.4.1.8 Fault Hazard Analysis (FHA) The FHA is very similar to a PHA. It is a subset of the Failure Modes and Effects Analysis (FMEA) technique. The FHA is a basic inductive analysis that is used to perform an evaluation that starts with the most specific form of the system and integrates individual examinations into the total system evaluation. The purpose of the FHA is to systematically examine a facility or system and to identify hazards and their effects. (See FMEA)

2.4.1.9 Material Compatibility Analysis Material Compatibility Analysis provides an assessment of materials utilized within a particular design. Any potential degradation that can occur due to material incompatibility is evaluated. System Safety is concerned with any physical degradation due to material incompatibility that can result in contributory hazards or failures which can cause mishaps to occur.

2.4.1.10 Procedure Analysis Procedure Analyses are often designated by the procedure or activity to be analyzed, i.e., Test Safety Hazard Analysis, Operation Safety hazard Analysis, Maintenance Safety Hazard Analysis, Job Safety Analysis. The Procedure Analysis provides an analysis technique to perform step-by step reviews of procedures in operations to detect the possibilities of:

- harm to operations by the system/subsystems, or
- harm to the system/subsystems by the operators.

2.4.1.11 Process Hazard Analysis A Process Hazard Analysis is a requirement of OSHA 1910.199 (29 CFR 1910.199) for the management of highly hazardous chemicals. It is a means of identifying and analyzing the significance of potential hazards associated with the processing or handling of certain highly hazardous chemicals.

2.4.2 Subsystem Hazard Analysis (SSHA) The SSHA is performed to identify and document hazards associated with the design of subsystems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and assemblies within the subsystems as well as their external interfaces. It includes software whose performance, degradation, functional failure or inadvertent functioning could result in a hazard. It also includes a determination of the modes of failure including reasonable human errors, single point failures and the effects on safety when failures occur within subsystem components and assemblies.

As with the SHA, specialized analysis will be used to support or complement the SSHA. Some of the most common specialized analyses are:

2.4.2.1 Cable Failure Matrix Analysis (CFMA) The CFMA is a shorthand method used to concisely represent the possible combinations of failures that can occur within a cable assembly.

2.4.2.2 Common Cause Analysis The purpose of the common cause analysis is to identify any accident sequences in which two or more events could occur as the result of a common event or causative mechanism. If the probability of a common cause is significantly greater than the probability of two or more events occurring independently, then the common cause could be an important risk contributor. These single secondary cause/events may result from a common process, manufacturing defect, a common human operator error, or some common external event. This technique is very useful for accident reconstruction.

2.4.2.3 Petri Net Analysis The purpose of the Petri Net Analysis is to provide a technique to model systems components at a wide range of abstract levels. Once a Petri Net model has been developed, its mathematical representation can be analyzed by automated means. The analysis can be used to model an entire system, subsystems, or system components at a wide range of abstract levels all the way through conceptual, top level and detailed designs, down to actual implementation in hardware and software.

2.4.2.4 Human Error/Factors Analysis

2.4.2.4.1 Human Error Analysis This analysis is used to identify the systems and the procedures of a process where the probability of human error is of concern. The concept is to define and organize the data collection effort such that it accounts for all the information that is directly or indirectly related to an identified or suspected problem area. This analysis recognizes that there are, for practical purposes, two parallel paradigms operating simultaneously in any human/machine interactive system one comprising the human performance and the other, the machine performance. The focus of this method is to isolate and identify, in an operational context, human performance errors that contribute to output anomalies and to provide information that will help quantify their consequences.

2.4.2.4.2 Human Factors Analysis The Human Factors concept is the allocation of functions, tasks, and resources among humans and machines. The most effective application of the human factors perspective presupposes an active involvement in all phases of system development from design to training, operation and, ultimately, the most overlooked element, disposal. Its focus ranges from overall system considerations (including operational management) to the interaction of a single individual at the lowest operational level. However, it is most commonly applied and implemented, from a systems engineering perspective, to the system being designed and as part of the SHA.

2.4.2.5 Sneak-Circuit Analysis (SCA) The purpose of the SCA is to identify unintended paths or control sequences that may result in undesired events or inappropriate timed events. It is accomplished by examining circuits (or command/control functions), searching out unintended paths (or control sequences) which, without component failure, can result in undesired operations, or in desired operations at inappropriate times, or which can inhibit desired operations. SCA is applicable to control and energy-delivery circuits of all kinds, whether electronic/electrical, pneumatic, or hydraulic and is adaptable to software analysis.

2.4.2.6 Structural Safety Analysis Is used to validate mechanical structures. Inadequate structural assessment results in increased risk due to the potential for latent design

problems causing structural failures, i.e., contributory hazards. Structural design is examined via mathematical analysis to satisfy two conditions:

- Equilibrium of forces, and
- Compatibility of displacements

The structure considered as a whole must be in equilibrium under the action of the applied loads and reactions; and, for any loading, the displacements of all the members of the structure due to their respective stress-strain relationships must be consistent with respect to each other.

2.4.2.7 The Human Error Rate Prediction (THERP) The purpose of THERP is to provide a quantitative measure of human operator error in a process and is a means of quantitatively estimating the probability of an accident being caused by a procedural error.

2.4.2.8 Test Safety Analysis (TSA) TSA is used to ensure a safe environment during the conduct of systems and prototype testing. It also provides safety lessons to be incorporated into the design, as applicable. Each test is evaluated to identify hazardous materials or operations.

2.4.2.9 Time/Loss Analysis (T/LA) for Emergency Response Evaluation Is a system safety analysis-based process developed to semi-quantitatively analyze, measure and evaluate planned or actual loss outcomes resulting from the action of equipment, procedures and personnel during emergencies or mishaps. T/LA procedures produce objective, graphic time/loss curves showing expected versus actual loss growth during emergencies or mishaps. The expected versus actual loss data is used to describe the change in the outcome produced by intervention actions at successive states of the emergency response. Although it is a system level analysis, due to lack of design definition and maturity, it is not usually initiated until after the SSHA has begun and uses the SSHA data before it is integrated into the SHA.

2.4.3 Software Hazard Analysis (SWHA) The SWHA identifies hazardous conditions incident to safety critical operator information and command and control functions identified by the PHA, SHA, SSHA and other efforts. It is performed on safety critical software-controlled functions to identify software errors/paths which could cause unwanted hazardous conditions. The SWHA can be divided into two stages, preliminary and follow-on.

2.4.3.1 Preliminary SWHA The Preliminary SWHA is used to examine software design to identify unsafe inadvertent command/failure-to-command modes for resolution. It is accomplished by tracing safety critical operator information and commands through flow charts, storage allocation charts, software and hardware specifications and other applicable documentation.

2.4.3.2 Follow-on SWHA This phase of the SWHA examines software and its system interfaces for events, faults, and occurrences such as timing which could cause or contribute to undesired events affecting safety. It is accomplished by tracing safety critical

operator information and commands through source/object code by system simulation. Safety critical programs/modules are analyzed for sensitivity to software or hardware failures which could cause the system to operate in a hazardous manner.

Specialized analysis used to support or complement the SWHA are:

2.4.4 Operating and Support Hazard Analysis (O&SHA) The purpose of the O&SHA is to examine procedurally controlled activities and to identify hazards and recommend risk reduction alternatives during all phases of intended system use. This analysis identifies and evaluates:

a. Activities which occur under hazardous conditions, their time periods, and the actions required to minimize risk during these activities/time periods.
b. Changes needed in functional or design requirements for system hardware/software, facilities, tooling, or S&TE to eliminate hazards or reduce associated risk.

c. Requirements for safety devices and equipment, including personnel safety and life support and rescue equipment.

d. Warnings, cautions, and special emergency procedures.

e. Requirements for PHS&T and the maintenance and disposal of hazardous materials.

f. Requirements for safety training and personnel certification.

While many of the analyses initiated during the PHA, SHA and SSHA are carried over and integrated into the O&SHA, the following specialized analysis are used to support or complement the O&SHA are:

2.4.4.1 <u>Accident Analysis</u> The purpose of the Accident Analysis is to evaluate the effect of scenarios that develop into credible accidents. Those that do not develop into credible accidents are documented and recorded to verify their consideration and validate the results.

2.4.4.2 <u>Confined/Enclosed Space Safety Analysis</u> The purpose of this analysis is to highlight the type of systematic examination of confined space hazards that should be conducted in order to preclude or at least minimize the potential for accidents.

2.5 DEPLOYMENT, AND OPERATIONAL PHASES

The SHA, SSHA, SWHA and O&SHA are all carried over into the Deployment and Operational Phases. Depending upon system complexity, the SHA, SSHA and SWHA may all be rolled into and carried forward as a single integrated O&SHA which will be initiated during the latter portion of the Design Phase. As the basic system is changed, modified and upgraded, various supporting analysis will be reapplied to ensure the integrity and currency of the existing Safety Risk Assessments.

2.6 DISPOSITION PHASE

Some or all of the previously discussed analyses may be carried forward and revised, initiated or reinitiated just prior to transitioning from the Operational to the Disposition Phase:

- Accident Analysis
- Common Cause Analysis
- Cryogenic Systems Safety Analysis
- Environmental Risk Analysis
- Fire Hazard Analysis
- Human Error/Factors Analysis
- Laser Safety Analysis
- Materials Compatibility Analysis
- Nuclear Safety/Cross-Check Analysis[4]
- Probabilistic Risk Assessment
- Process Hazard Analysis
- Structural Safety Analysis
- Change Analysis
- Confined/Enclosed Space Safety Analysis

However, the Deactivation Safety Analysis is specifically applicable to the Disposition Phase.

Deactivation Safety Analysis The purpose of the Deactivation Safety Analysis is to identify significant safety and health (S&H) concerns integral to the deactivation process. The S&H practices are applicable to all deactivation activities, particularly those involving systems or facilities that have used, been used for, or have contained hazardous or toxic materials. The deactivation process involves placing the system or facility into a safe and stable condition that can be economically monitored over an extended period of time while awaiting final disposition for reuse or disposal. The deactivation methodology emphasizes specification of end-points for cleanup and stabilization based upon whether the system or facility will be deactivated for reuse or in preparation for disposal. Specific guidance or procedures can be found in the following documentation:

- DOE Order 5480.23 Nuclear Safety Analysis Reports
- DOE Order 5481.1B Safety Analysis and Review System
- DOE Order 6430.1A General Design Criteria

Supporting References include:

- DOE-STD-1027-92
- DOE-STD-3009-94
- DOE-STD-3011-94

[4] Nuclear powered systems only.

- DOE/EM-0318-96
- DIE/EH-0486-92

Although these documents are primarily geared towards the Nuclear Power Industry, it should be remembered that Nuclear waste is, in fact, one among many hazardous materials and another form of toxic waste.

2.7 INPUT ANALYSIS

There are other evaluation procedures and system analyses which are routinely conducted by other Systems Design, Engineering, and Integration functions, such as Reliability & Maintainability Engineering, upon which system safety depends for vital input data. Conversely, some of those evaluations/analyses use data provided from system safety analysis. Some of theses analyses are:

2.7.1 Failure Modes, Effects and Criticality Analysis (FMECA) The FMECA is an essential function in design from concept through development. The FMECA documents all probable failures of a system within specified ground rules, determines by failure modes analysis the effect of each failure on system operation, identifies single failure points, and ranks each failure according to a severity classification of failure effect. The methodology is the result of the following two analysis steps which, when combined, produce the FMECA:

2.7.1.1 Criticality Analysis The purpose of the criticality analysis is to rank each potential failure mode identified in a FMEA according to the combined influence of severity classification and its probability of occurrence based on the best available data.

2.7.1.2 Failure Modes and Effects Analysis (FMEA) The purpose of the FMEA is to determine the results or effects of sub-element failure on a system operation and to classify each potential failure according to its severity.

2.7.2 Damage Modes and Effects Analysis (DMEA) The purpose of the DMEA is to provide early criteria for survivability and vulnerability assessments. The DMEA provides data related to damage caused by specified threat mechanisms and the effects on system operation and mission essential functions.

2.7.3 Digraph Utilization Within System Safety Directional Graphs (digraphs) have been used to model failure effect scenarios within large complex systems, thereby modeling FMEA data. Digraphs can also be used to model hazardous events and reconstruct accident scenarios. As a result, both hazard analysis and accident investigation processes can be improved via modeling event sequences.

2.7.4 Electromagnetic Compatibility (EMC) Analysis and Testing EMC analysis is conducted to minimize/prevent accidental or unauthorized operation of critical safety functions within a system. The output of radio frequency (RF) emitters can be coupled into and interfere with electrical systems which process or monitor critical safety functions. Electrical disturbances may also be generated within an electrical system from

transients accompanying the sudden operation of electrical devices. Design precautions must be taken to prevent electromagnetic interference (EMI) and electrical disturbances. Human exposure to electromagnetic radiation is also a concern.

2.7.5 Energy Trace and Barrier Analysis (ETBA) for Hazard Discovery and Analysis The ETBA method is a system safety-based analysis process developed to aid in the methodical discovery and definition of hazards and risks of loss in systems by producing a consistent, detailed understanding of the sources and nature of energy flows that can or did produce accidental harm. Outputs support estimation of risk levels, and the identification and assessment of specific options for eliminating or controlling risk.

These analyses are routinely started in conjunction with the SHA and may be initiated when critical changes or modifications are made.

2.8 DECISION ANALYSES

The following decision analyses are analysis tools and techniques primarily used by System Safety Management:

2.8.1 Control Rating Code (CRC) Method The CRC method is a generally applicable system safety-based procedure used to produce consistent safety effectiveness rating of candidate actions intended to control hazards found during system safety analyses or accident investigations. Its primary purpose is to control recommendation quality. A secondary purpose is to require systematic application of accepted safety principles to the identification and selection of hazard controls intended to control system risk. Finally, it helps analysts identify priorities to support specific hazard control action plans.

2.8.2 Critical Path Analysis (CPA) The CPA and Program Evaluation Review Technique (PERT) are the two most commonly used forms of Network Modeling and Network Analysis Techniques (NATs) which are utilized to manage large Complex Programs and Projects. A program or project network is basically a graphical representation or description of activities or milestones which are needed in order to solve a problem. By employing NATs (e.g., logic diagrams) solutions can be obtained for a particular problem. PERT has been used to assist management in planning and controlling many programs and projects that consist of numerous specific tasks (activities), each of which must be completed in order to complete the entire project.

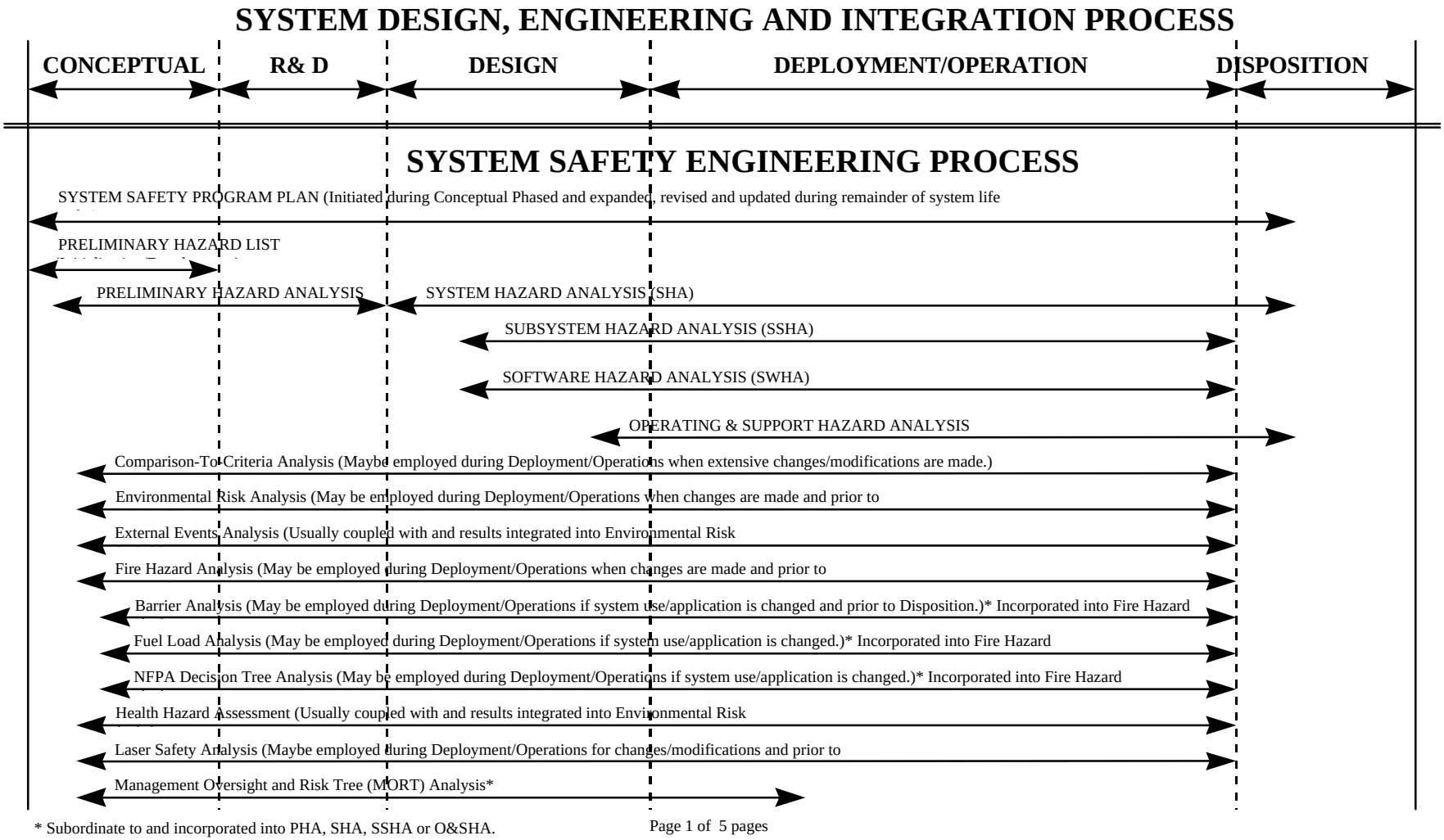
These analyses are routinely begun when the SSPP is initiated and revised throughout the system life cycle on an as needed as required basis.

2.9 SUMMARY

All of the available analyses have not been identified and not all of those identified will be applied during a specific System Safety Analysis Process. Just as the design is tailored to meet operational and cost goals and constraints, so too will the Process and corresponding analyses.

Figure 1

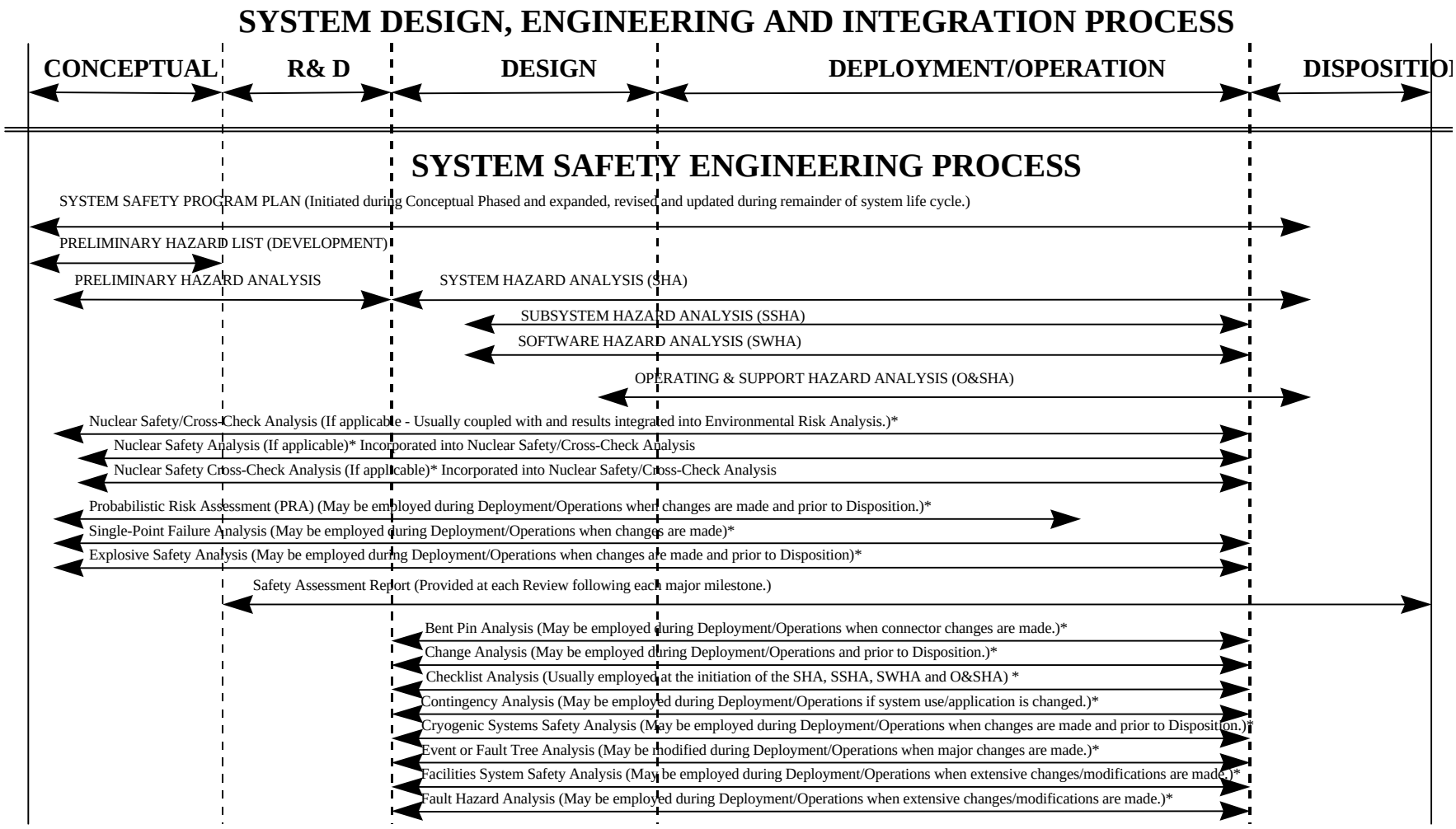
SYSTEM SAFETY ENGINEERING PROCESS



* Subordinate to and incorporated into PHA, SHA, SSHA or O&SHA.

Page 1 of 5 pages

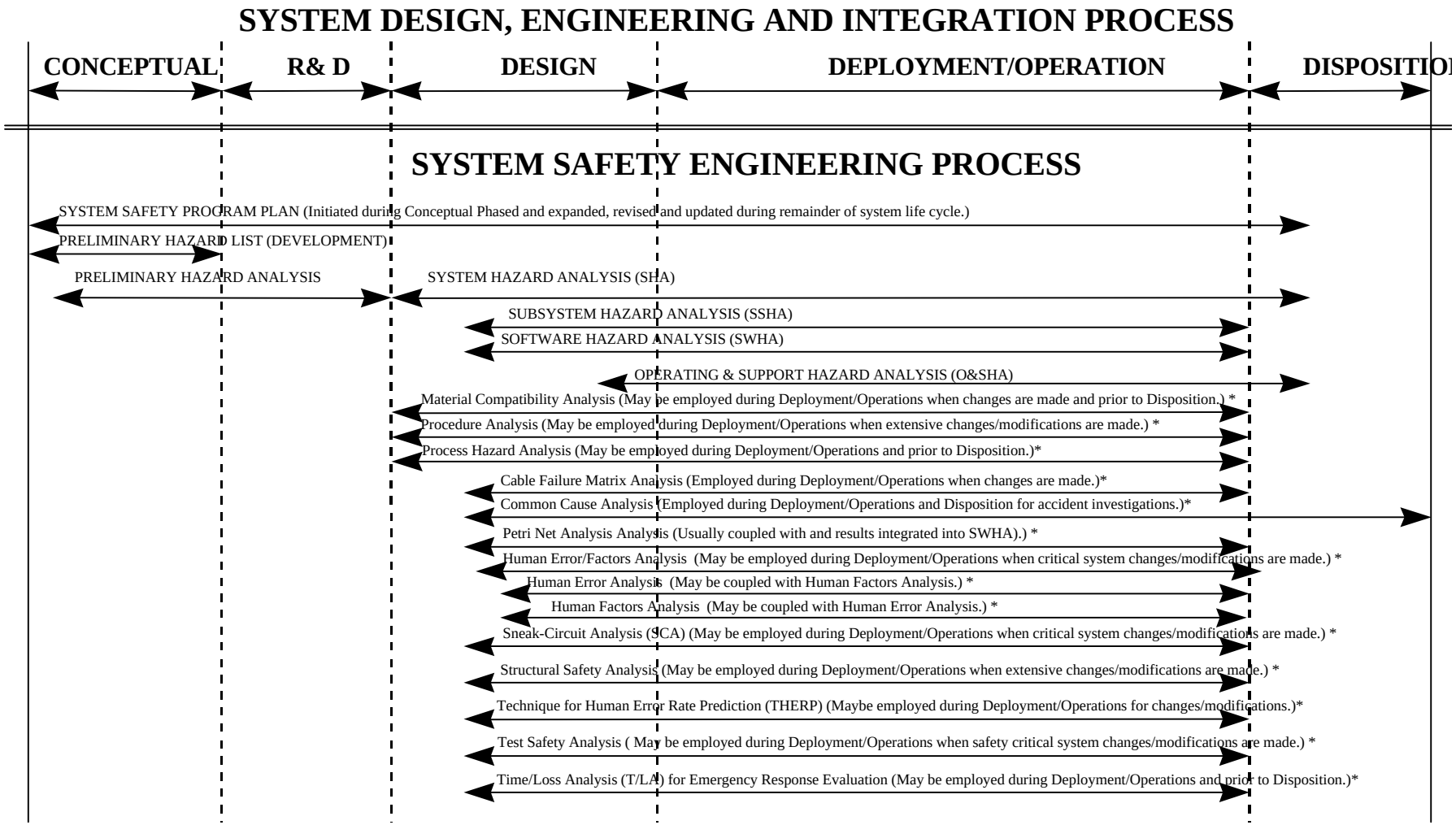
SYSTEM SAFETY ENGINEERING PROCESS



* Subordinate to and incorporated into PHA, SHA, SSHA or O&SHA.

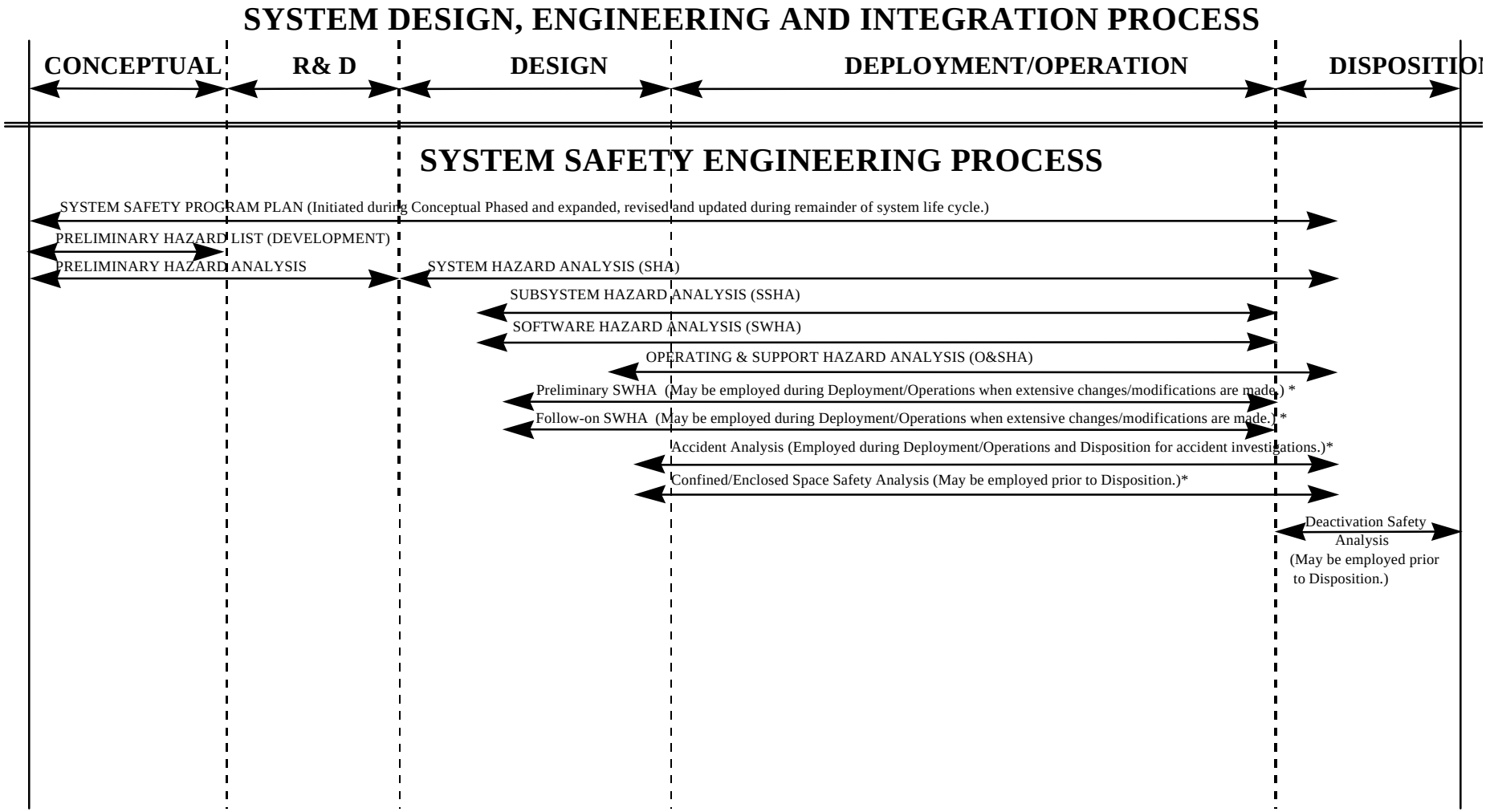
Page 2 of 5 pages

SYSTEM SAFETY ENGINEERING PROCESS



* Subordinate to and incorporated into PHA, SHA, SSHA or O&SHA.

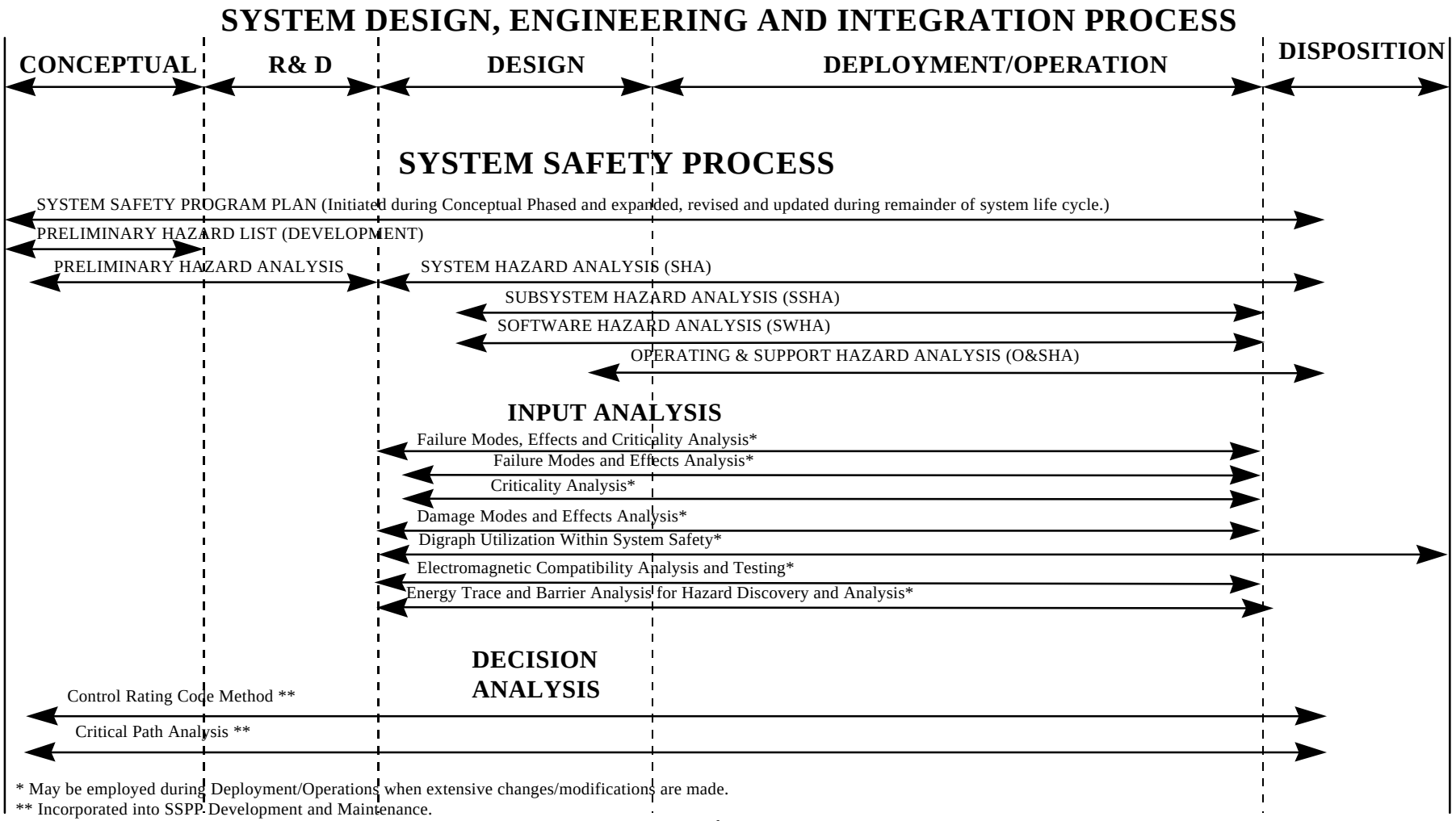
SYSTEM SAFETY ENGINEERING PROCESS



* Subordinate to and incorporated into PHA, SHA, SSHA or O&SHA.

Page 4 of 5 pages

SYSTEM SAFETY ENGINEERING PROCESS



Page 5 of 5 pages

Attachment 2

Application of Expected Casualty to Commercial Space Transportation

Introduction

Expected casualty is widely used in the commercial space transportation industry as a measure of risk, but often misunderstood. Simply put, it is "the expected average number of casualties per launch of a launch vehicle." Most people understand what an average is. To get this kind of average, one could conduct a large number of launches of a launch vehicle, add up the number of casualties, and divide by the number of launches.

The confusion seems to arise because expected casualty is not an actual average, but an "expected" average because the past number of launches of any one launch vehicle is too small to be statistically meaningful. Confusion also seems to arise because of how expected casualty is used - to measure risk prior to a launch. This paper describes the use of expected casualty as a measure of risk, the basic steps for applying expected casualty, real-world complications and the use of risk thresholds, the data needed to calculate expected casualty, and related concepts such as risk aversion and insurance values.

Expected casualty and risk

Expected Casualty is a measure of risk. The launch industry uses expected casualty to measure the risk to the public from a single launch (mission). Expected Casualty is one of the measures used to determine whether a launch can proceed.

The safety community defines risk (R) as the product of the probability (p) or frequency of occurrence (f) of an event, and its consequence (C) (the severity of its impact).[1] While the probability or frequency is always a fraction between 0 and 1, the measure of consequence can be any positive or negative number. Therefore the value of risk (R) can be any positive or negative number[2]. For risk, then, the larger the number, the greater the risk.

Driving a car provides a good example. Suppose there is a 10% chance that your car will receive $1000 in damage in driving from here to New York City, and a 90% chance that it will not receive any damage. The risk measure is $100 (.10 X $1000) for the trip.

Risk can be relatively high if the probability (p) of the event is close to 1.0 (high) and it can be relatively high if the consequence (C) is extremely great, even if the probability (p) is small. Risk can be made low by reducing the probability of an event with high consequences. This could be achieved by, for example, having a very reliable vehicle such that the probability of success is very high making the probability of casualty-causing

[1] Hazard Analysis of Commercial Space Transportation, Office of Commercial Space Transportation, Department of Transportation, 1988.

[2] In this context, a negative risk can be considered to be a "good" outcome since risk is generally considered in a negative context.

failure events very low. Risk can also be made low by reducing the consequences of failure events. This could be achieved by, for example, designing a launch vehicle whose failure events cause few casualties. This latter case is most consistent with current ELV operations. Launches take place over the ocean so the consequences of a failure are near zero even though the probability of a failure may be relatively high (10% or more).

Expected casualty for a mission measures the risk of conducting the mission and includes all the contributions to risk as a result of the mission. Those "possible" but extremely unlikely events (e.g., unique combination of launch events leading to the destruction of a nuclear power plant) are weighted appropriately in the risk context by the product of the probability and the consequence. This is shown in the example calculation below.

Example calculation #1: Assume that for a given proposed mission, there is a 60% chance of no casualties, a 30% chance of one casualty, and 10% chance of 3 casualties. We have accounted for all possible outcomes (100%). The complete equation for expected casualties is the sum, over all possible events, of the product of the associated probability, p_i, times its consequence, C_i.

$$E_c = \sum_{i=1}^{n} p_i \, x \, C_i$$

Where,
n = the number of possible different events
p_i = the probability of the i^{th} event, and $p_1 + p_2 + p_3 + \ldots + p_n = 1$,
C_i = the consequence of the i^{th} event

The risk of the mission, measured by Expected Casualty is (0.60 x 0) + (0.30 x 1) + (0.10 x 3) = 0.6. If plans were to launch 1000 times, we would "expect" a total of approximately 600 casualties. The "actual" number of casualties after actually conducting 1000 launches may be something like 590. The actual number will not necessarily equal the expected casualty.[3]

Basic steps for applying expected casualty

In applying the concept of expected casualty to a launch mission, it would be desirable to have already conducted hundreds or thousands of flights with the vehicle, particularly flights of the vehicle along the proposed flight path. One could count the type and time in flight that the failures occurred or, if thousands of flights were conducted along the proposed flight path, count the casualties. The job would be done. This is not realistic,

[3] A simple analogy is to use expected "value" to estimate the number of Heads that would be seen after flipping a coin 100 times. The answer would be the probability of a head on each flip (0.5) times the number of flips (100) for an expected value of 50. If one actually were to conduct such an experiment, the actual number of Heads might be close to but not exactly 50, because of chance. The more flips, however, the closer the ratio of Heads to total number of flips is likely to be to 0.5.

however, because: (1) the purpose of risk analysis is to verify that launch vehicle flights can be conducted with low risk of exposure to the public, so there is not likely to be data on casualty counts, and (2) launch vehicles, particularly new vehicles, have not had enough flights to provide enough vehicle failure data to be helpful (See Data For Expected Casualty below).

We instead use a basic process that involves categorizing all the events that might occur, their probabilities, and their consequences.

Events. One possible outcome is that the flight is a success and the consequence (casualties) associated with that event is 0. Another possible outcome is that while the flight is not a success (the vehicle may develop any number of problems), it is able to successfully abort the mission and return safely to the launch site or land at an alternative site. Again the number of casualties associated with this event is 0 if the sites are free of people. Finally, there may be a class of outcomes where the vehicle fails in such a way that the vehicle or debris will land or impact somewhere other than designated safe landing locations. Only the failure scenarios contribute to risk and expected casualty because the consequences associated with success and successful abort are 0.

The time in a flight when a failure event occurs is an important factor. For a given flight path, the time of failure (i.e. the location on the flight path) will not only affect the population that might be in the area of impacting debris, but may also affect the type of failure and the consequences of the failure (i.e. the amount or distribution of debris due to factors such as stages having been safely released prior to the event).

Probabilities. The second step is to determine the probability that each of the possible events will occur at various points in the flight?[4] To add the probability or frequency of each possible outcome, we could start with the probability of success (p_s), the probability of some type of failure which results in a successful abort (p_a), and the probability of failure (p_f). For sample problem #2 below, we will say that p_s is .95, p_a is .03 and p_f is .02. All the possible events have been addressed since these add to 1.0.

If there is an estimate of the failure probability for a vehicle or stage of a vehicle, and we assume the probability of failure is uniform throughout the flight path (i.e. the vehicle or stage will be no more or less likely to fail at any particular time in its flight), then the flight can be broken down into those flight times where population density is roughly the same[5].

[4] For some vehicles, the chance the vehicle will fail may be uniformly distributed along the flight path (e.g., a vehicle with a failure probability of .02 and a flight of 1200 seconds would have a likelihood of failing in any given second of .02/1200 or 1.67×10^{-5}). Other vehicles may have particular points along the flight path where the likelihood of failing is greater, such as at stage separations and the starting or restarting of engines. Thus the distribution of failure probability may be made up of a combination of certain numbers at certain locations and uniformly distributed for other segments of the flight. All probabilities for the failure events should add to the overall failure probability of the vehicle and the sum of all probabilities (including success and successful abort) should add to 1.0.

[5] This approach can be carried to extremes by dividing the exposed flight path up into an almost infinite number of areas. One way to avoid this is to pick larger areas which do not have a homogenous population density and assume the entire area as the largest population density found within the area. All other things being equal, this would result in a conservative estimate for expected casualty.

The relative time a flight profile exposes a given area is often referred as "dwell time." For example, if the overall probability of failure of a vehicle (or stage) is .02 and it exposes a specific area for 3 seconds out of a 6 minute flight, then the probability of failing such that debris will fall in that particular area is:

$$.02 \times (3 \text{ sec.}/300 \text{ sec.}) = 2 \times 10^{-4}$$

The above example is for a particular area. All the other areas would also need to be addressed. From the above example, there are still 297 seconds of the 300 seconds of flight that would need to be addressed. Note that when this is done, all portions (i.e., 100%) of the .02 failure probability will have been included.

Consequences. Another dimension of the problem is the need to determine the number of casualties (consequences), given that an event occurs. For the failure scenarios the consequences depend on a number of factors, including the time in the flight that the failure occurs, the density of population in the area where debris impacts, and the type of failure (e.g. explosion, loss of thrust, etc.). This is also a probabilistic problem because the same event will not always cause the same consequence. However, there is a commonly accepted approach which determines the "average" expected consequence.

Assume an event "i" causes debris to fall into populated areas. The consequence is determined based on the number of people expected to be within the "total casualty area" of the launch vehicle debris generated. The casualty area for each individual piece of debris is the area within which 100 percent of the unprotected population on the ground is a casualty due to debris impact. The total casualty area is the summation of the casualty areas of each piece of debris. Casualty area is based on the size of a standing person and a launch vehicle's debris characteristics at particular points on its trajectory. The debris characteristics include fragment size, path angle of the fragment trajectory, fragment impact explosions, and fragment slide, bounce, and scatter.[6]

There are relatively straightforward processes for determining the casualty area from debris characteristics. In order to simplify the process, assume the debris is inert (e.g., a non-explosive piece of debris) and is falling straight down. In this case, 2 feet is added to the largest cross sectional diameter of the debris, to account for the size of a standing person. This becomes the radius of a circle which defines the casualty area for that piece of debris. This is done for each piece of debris, the characteristics of which could cause a casualty if it hit a person. All the areas are summed to provide the casualty area, A_{ci}, for the ith event.

The casualty estimation is simply the population density, D_p (people per square mile), times the casualty area of the debris, A_c (square miles). That is:

$$C_i = D_{pi} \times A_{ci},$$

[6] The determination of the debris characteristics is routinely performed for ELVs and should present no greater problem for RLVs.

Where:
C_i = the consequence of the i^{th} event,
D_{pi} = the population density of the area exposed by the i^{th} event, and
A_{ci} = the casualty area of the debris generated by the i^{th} event.

Without the simplifications of having inert debris falling straight down, the above process would have to be modified to account for a number of factors. First, if the debris has a horizontal velocity component, the radius is expanded to account for the lateral movement of the debris as it passes from a height of 6 feet (assumed height of a person) to the ground. Second, if the debris is likely to shatter or cause harmful objects to be sprayed outward on impact, this distance is added to the cross sectional diameter of the object. Third, if the debris may explode on impact, equations exist which can determine the distance from the debris at which the overpressure would not exceed .5 pounds per square inch.[7] Lastly, adjustments for bounce and slide of debris may also be necessary, which can increase the casualty area by a factor of 3 to 4.[8]

There are other approaches for calculating casualty areas, but all boil down to the same basic principles. Some may be of "high fidelity" such as using Monte Carlo techniques to model the individual impact locations and distribution (i.e., develop a map of p_i contours) of the impacting debris by various classes (e.g., size, explosive nature, etc.). Such an approach might be used, for example, when the debris pattern is so large that it would extend into one or more areas of different population densities.

Example calculation #2: Following the process described above, we first breakdown the flight path into segments, and determine the probabilities of failure in each. For this example, we will say there are 4 areas in the flight profile within each of these areas the probability of failure, the population density and the debris casualty areas are the same.

1. The first area is in the immediate vicinity of the launch point. Of the .02 probability of a catastrophic failure, .01 will occur in this area, the debris casualty area is 5,000 square feet (1.79×10^{-4} square miles) and the population density is 0 (the area is cleared of people).
2. In area 2, of the .02 probability of failure, there is a .005 probability of failure, the casualty area is 4500 square feet (1.61×10^{-4} square miles) and the population density is 5 people per square mile.
3. In area 3, of the .02 probability of failure, there is a .004 probability of failure, the casualty area is 2000 square feet (7.17×10^{-5} square miles) and population density is 1000 people per square mile.

[7] An overpressure at or below 0.5 psi is considered safe for the general public.

[8] The process described above is conservative because it assumes that two pieces hitting the same individual results in two casualties. The likelihood of this happening is dependent on the population density and the degree to which the debris pieces are dispersed (i.e., how far apart they land from each other). A report entitled, Calculation of Expected Casualty By Three Methods, Lance A. Wheeler, Missile Flight Safety, White Sands Missile Range, NM, August 1996, notes that in some instances the resultant number of casualties can be significantly reduced because of multiple hits on the same individual.

4. In area 4, there is a probability of .001 of failure, the casualty area is 1000 square feet (3.59×10^{-5} square miles) and population density is 5000 people per square mile.

Note that we have now accounted for all the events for the flight. If we add the probabilities for each possibility, we get 1.0. Each possibility is exclusive of the other (i.e., there will be one outcome).[9] Going to the equation for Expected Casualty, the Expected Casualty for the example flight can be determined.

$$E_c = p_s \times 0 + p_a \times 0 + \sum_{i=1}^{4} p_i \times D_{pi} \times A_{ci}$$

$$E_c = .95 \times 0 + .03 \times 0 + .01 \times 0 \times 1.79 \times 10^{-4} + .005 \times 5 \times 1.61 \times 10^{-4} + .004 \times 1000 \times 7.17 \times 10^{-5} + .001 \times 5000 \times 3.59 \times 10^{-5}$$

$$E_c = 4.70 \times 10^{-4}$$

Real world complications and the use of risk thresholds

All the basic elements for the determining the expected casualty for a mission are covered above. In the real world, however, the process is more complicated due to the following real world complications:

1) The process needs to cover a great number of possible events.
   - There are likely to be many different failure modes that could affect the characteristics of the debris and casualty area.
2) If a launch vehicle flies a considerable distance over land, a large number of population areas must be addressed.

Luckily, however, the goal in the real world is not to determine the actual risk, but to determine that the risk is below a certain threshold. This allows one to avoid complications noted above by making conservative assumptions or assuming worse case scenarios. For example, if different failure modes affect the same population, one may wish to simply base the consequences of all failure modes on the worst case. To decrease the number of populated areas, one may take a large area with a mix of population densities, and simply assume the entire area consists of the highest population density.

The process of demonstrating that the Expected Casualty is less than or equal to some threshold number, without knowing the actual risk, provides assurance to a safety organization that the risks are acceptable. If, however, the derived number is greater than

[9] An analogy is a "wheel of fortune" with large spaces around edge of the wheel taken up by some of the numbers and smaller spaces taken up by other numbers. It is more likely to stop at those numbers taking up more of the space around the wheel's perimeter. The wheel encompasses 360 degrees and the number of degrees taken up by a certain space on the wheel reflects the probability that the wheel will stop on that space (i.e., the probability = number of degrees taken up by the space/360 degrees). Yet when the wheel is spun it will eventually stop only at one of the numbers.

the threshold number, it would may be necessary to go back and perform a "higher fidelity" analysis making less conservative assumptions.

One "higher fidelity" approach for determining expected casualties than those discussed above is a Monte Carlo simulation. Such approach is a mathematical version of the example "wheel of fortune" model. Here individual flights are "flown" by the model hundreds or thousands of times and the resultant casualties of each "flight" recorded. The advantages of the simulation approach is that such models can easily handle the many different events that could occur and can give a "higher fidelity" answer. This is particularly important when the assumptions used above result in an answer that exceeds the threshold (e.g., expected casualty is equal to or less than 90×10^{-6} and the threshold is 30×10^{-6}). This more refined approach could show that the expected casualty is indeed less than the threshold.

Data for expected casualty

For a launch operator to determine all the events that might occur, their probabilities, and their consequences, the launch operator needs to obtain data such as population data, launch vehicle effective casualty areas, and vehicle failure rates. Population information can be straightforward if census data is available. Determining the effective casualty area of a launch vehicle at particular points on its trajectory is also a straightforward process using accepted procedures.

The development of vehicle failure rates is more involved. The failure rates for the vehicle are driven by the failure rates and modes of major systems. These in turn are driven by the failure rates and modes of the subsystems. There are standard engineering analysis techniques for deriving estimates of these rates such as Failure Modes and Effects Analysis and Fault Tree Analysis.[10]

As noted above, however, without a great deal of experience with the specific systems and subsystems, such analyses will produce only rough estimates of the likelihood of various types of failures or, alternatively, the mean time between failures. The more performance and reliability experience one has on subsystems and components, the more accurate one's estimate would be. Unlike aircraft, where there have been hundreds of thousands of aircraft systems (e.g., jet turbine engines) produced and flown, launch vehicles and particularly many of the proposed reusable launch vehicles do not have major systems with much flight history.

Luckily, although many of the major systems of a launch vehicle are likely unique, many of the subsystems and components do have performance and reliability experience. The usefulness of the experience is dependent on whether the subsystem or component was

[10] On average based on a recent review of the flights of new expendable launch vehicles, approximately 30% of the first series of launches (i.e., launches 1 through 3) fail. This is often a higher failure rate that would be otherwise indicated by the analytical methodologies. The difference is believed to be because all failure modes are not identified in the analyses or their likelihood is determined to be lower than may be the case.

used in a similar environment and whether the interfaces and interactions between subsystems/components was similar.

Regardless of the amount of performance and reliability experience one has on a launch vehicle, some kind of test program is necessary to provide confidence in the performance of critical systems. While many tests can be conducted on a system level while on the ground (e.g., much like turbine engine test stands for testing aircraft engines after a major overhaul), it is necessary to conduct flight tests in order to test all the systems and their interactions in a flight environment. Even new aircraft typically go through a flight test program during which the functioning and performance of the aircraft and systems are checked out in a flight environment before they may fly over densely populated areas.

Related concepts

Risk aversion. Risk aversion is also a factor in the concept of risk and decision making. There are often certain types of consequences which are simply not acceptable, or at least carry more weight than other consequences.[11] Under these circumstances one might consider eliminating the possibility of the high consequence event by preventing the exposure from occurring in the first place. For example, this might be done by not allowing a launch vehicle to fly over (and expose) areas with extremely high population densities.

Such an action certainly eliminates the possibility of a high consequence event. It does not, in and of itself, ensure that a specific expected casualty value will, or can, be achieved. In most instances, it likely means the expected casualty value will be reduced.[12]

Insurance. The amount of insurance a launch operator should obtain is determined by a process known as maximum probable loss (MPL). The same contributors to an expected casualty analysis for a mission is also often useful in a MPL analysis. Here the focus is what is the greatest probable loss. This too involves a threshold, but this threshold is a probability, not an expected casualty or loss number. The maximum probable loss is set such that there is no more than a given probability that losses will exceed some value, set in dollars.

[11] For example, while a low probability event with high potential consequences might have the same Risk as another higher probability event with less potential consequence (i.e. $p_1 \times C_1 = p_2 \times C_2$), it is possible that the high consequence event is unacceptable while the lower consequence event is acceptable. In other words, 10 accidents out of 100,000 flights involving 1 casualty each might generate less concern than the possibility of 1 accident in 100,000 flights involving 10 casualties even though they both have the same risk value and contribute the same to expected casualty, 1×10^{-4} (10/100,000).

[12] Unusual examples could be contrived where the avoidance of a high consequence area (e.g., city) might result in an overall increase in the mission's expected casualty. For example, say the dwell time over the city was 1 second and the failure rate is uniform at .0001 per second and the consequences would be 10, the contribution (i.e., the ith event) would be 1×10^{-3}. If avoiding the city would mean an additional flight time of 5 seconds which would be over an area with a population density such that the consequence would be 3, the contribution to expected casualty would be 1.5×10^{-3}. While the maximum consequence event has been reduced, the expected casualty number is actually increased in this example.

Sample calculation #3: Let us assume the MPL value is to be the number of losses which are to be exceeded with a probability of no more than a .005.[13] The probability of .005 is then the threshold used for "probable."

The simplest approach is to create a table of the losses, the probabilities of each loss, and the cumulative probability. The table will begin with the largest loss and work in descending order by loss because we are interested in the largest loss that will only be exceeded with a probability of .005. The Table is then:

Loss	Probability	**Cumulative Probability**
1795 ($5000 \times 3.59 \times 10^{-5}$)	.001	.001
.0717 ($1000 \times 7.17 \times 10^{-5}$)	.004	.005
8.5×10^{-4} ($5 \times 1.61 \times 10^{-4}$)	.005	.010
0	.01	.02

Looking at the cumulative probability column, there is a .01 probability that losses will exceed 8.5×10^{-4} and a .001 chance that losses will equal .1795. Therefore the MPL value would be .0717 as there is a probability of .005 that losses will equal or exceed .0717. Note also that the cumulative probability sums to .02 which is equivalent to the likelihood of some catastrophic failure during the mission.[14]

[13] It is important to understand that the numbers and definition for MPL used here are NOT those actually used but are provided here for the purpose of the exercise intended to show another view and use of the mission data in the context of casualties.

[14] One can actually test this or a similar example by building a wheel or developing simulation model driven by random numbers.